

トークンレス・ワンタイムパスワード

# PassLogic

エンタープライズ版

バージョンアップ概要とリリースノート(エンタープライズ版 v3.0.0)

2017/5/18



1. リリースノート
2. 機能アップ
3. 機能改善・不具合修正

# PassLogicの歩み

1987

「乱数表から抜き出してワンタイムパスワードを生成する」システム PassLogic 認証方式を発明。

2000-2006

パソロジック方式の技術ライセンスを日本企業へ提供。

2008

Webサービス組み込み用APIを強化。スマートデバイスにいち早く対応。



2010

セキュリティポリシーや運用機能、連携機能など基本機能を大幅に拡充。英語対応し海外展開が可能に。マルチテナント版リリース。

2012

マルチテナント版機能拡充しサービスプロバイダのデファクト採用の礎に！  
(ソフトバンク/富士通/KDDI/NEC/IIJなど)

70万ID突破

2015



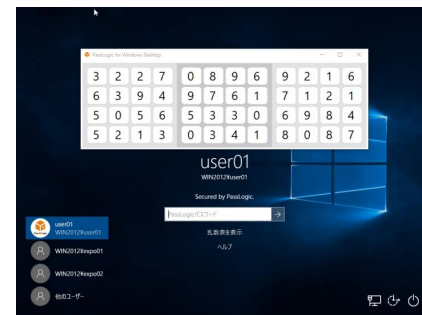
100万ID突破

エンタープライズ版の機能拡充。主要連携製品とメーカー間の検証を完了。ソフトウェアトークン提供開始

2017

IPアドレス制限、Windows ログイン、PKIに対応のメジャーバージョンv3.0リリース。

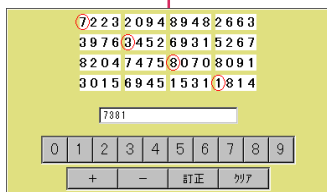
108万ID突破



2017

1987

2000



PassLogic認証方式が米国特許(US6141751)を取得。会社設立。

2007

PassLogicのパッケージ販売を開始。SSL-VPN連携機能を実装。

2009

Webアプリとの連携機能 (リバースプロキシ&SSO) を実装。LDAPからのユーザID同期を実装。

2011

クラウドアプリ連携 (SAML) に対応。スマートデバイス最適化。

2013

運用の自動化を実現する機能拡充。

80万ID突破

2014

小規模から大規模要件まで対応可能なエンタープライズ版をリリース。

90万ID突破



2016

利用者視点の機能強化を中心に、計5回のバージョンアップ、約70の機能追加・改善を実施。

PassLogic

# V2系のライフサイクルについて

PassLogic Ent v3.0のリリースに伴い、v2系のライフサイクルが下記の通りとなります。

| 対象バージョン                 | EoS            | EoL        |
|-------------------------|----------------|------------|
| PassLogic エンタープライズ版 v3系 | V4.0の提供開始から半年後 | EoSから5年後   |
| PassLogic エンタープライズ版 v2系 | 2017/11/18     | 2022/11/18 |
| PassLogic エンタープライズ版 v1系 | 2015/10/15     | 2020/10/15 |

メジャーバージョンアップ版は年間保守サポートサービスのなかでソフトウェアプログラムをご提供します。

EoS : End of Sales (販売終了)  
EoL : End of Life (サポート終了)

EoSは販売終了日の6か月以上前に公開情報として提供されます。  
(サイト上での情報提供を予定しております。)

# リリースノート

# リリースノート

## 【機能アップ】

- ・PKI機能（証明書発行・管理機能と認証連携機能）を追加しました。
- ・IPアドレス制限（WebAPP、Cloud連携）を追加しました。
- ・Windowsログイン機能（WindowsのAD連携ユーザのログイン時にPassLogic認証をする機能）を追加しました。

## 【機能改善・不具合修正】

- ・LDAP認証連携のLDAPサーバ冗長化対応しました。
- ・LDAP認証連携の際に利用できるADのユーザ名を小文字のみに限定できるようになりました。  
(Windowsは英字の大文字と小文字を区別しませんが、PassLogicでは区別して扱います。LDAPとのID連携時は、その違いにより問題が生じる可能性があるため本機能を有効にしてください。)
- ・WebTokenの乱数表表示前にUID入力画面を追加し、個別のWebTokenをユーザで指定して表示できるようになりました。
- ・一部SSL-VPN機器のSSOの際に、『特定URLにアクセスして取得するCookie』を要求する仕様に対応できるようになりました。
- ・SSL-VPN機器連携の際に、保存されたADパスワードをアトリビュートとして送信できるようになりました。
- ・リストアの際にDB情報と設定情報を個別にリストアできるように改善しました。
- ・冗長構成のリカバリ機能を最適化したことにより、アクセス停止時間を短縮しました。
- ・冗長構成で、リカバリ実行の際、ファイル管理されている設定情報をリカバリ先にコピーする・しないが選択可能になりました。
- ・冗長構成のリカバリ処理をコマンドラインから実行することが可能になりました。
- ・冗長構成時、ファイル管理されている設定情報を冗長先にコピーするコマンドが利用可能になりました。
- ・PassLogicの設定ファイル内に、メール設定のSMTP認証パスワードを暗号化して保存できるようになりました。
- ・パスワードリマインダーよりパスワードリセットした際、ユーザのロックも同時に解除するようになりました。
- ・アップロード可能なバックアップファイルサイズのデフォルト設定値が、16MB から128MB になりました。

## 【廃止機能】

- ・冗長構成でリカバリ処理終了時のfailback メール送信を廃止しました。
- ・ユーザー名、ドメイン名、ポリシー名、グループ名、smtpサーバ名、radius クライアント名に、単一文字"0" が利用できなくなりました。

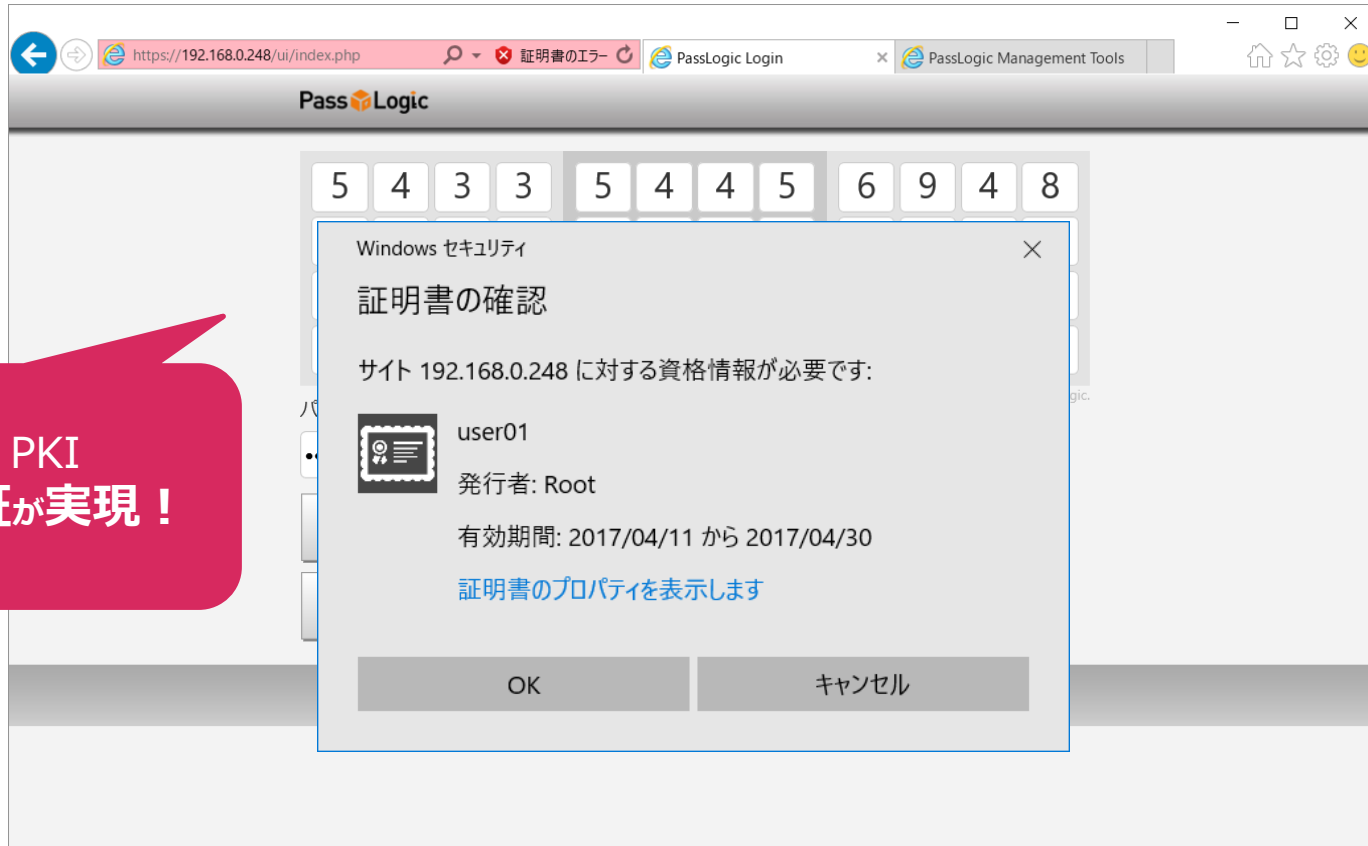


The background features a teal and light blue geometric pattern of overlapping squares and rectangles, creating a sense of depth and movement. The pattern is centered horizontally and vertically, with the text overlaid in the middle.

機能アップ

# PKI機能（2要素認証）

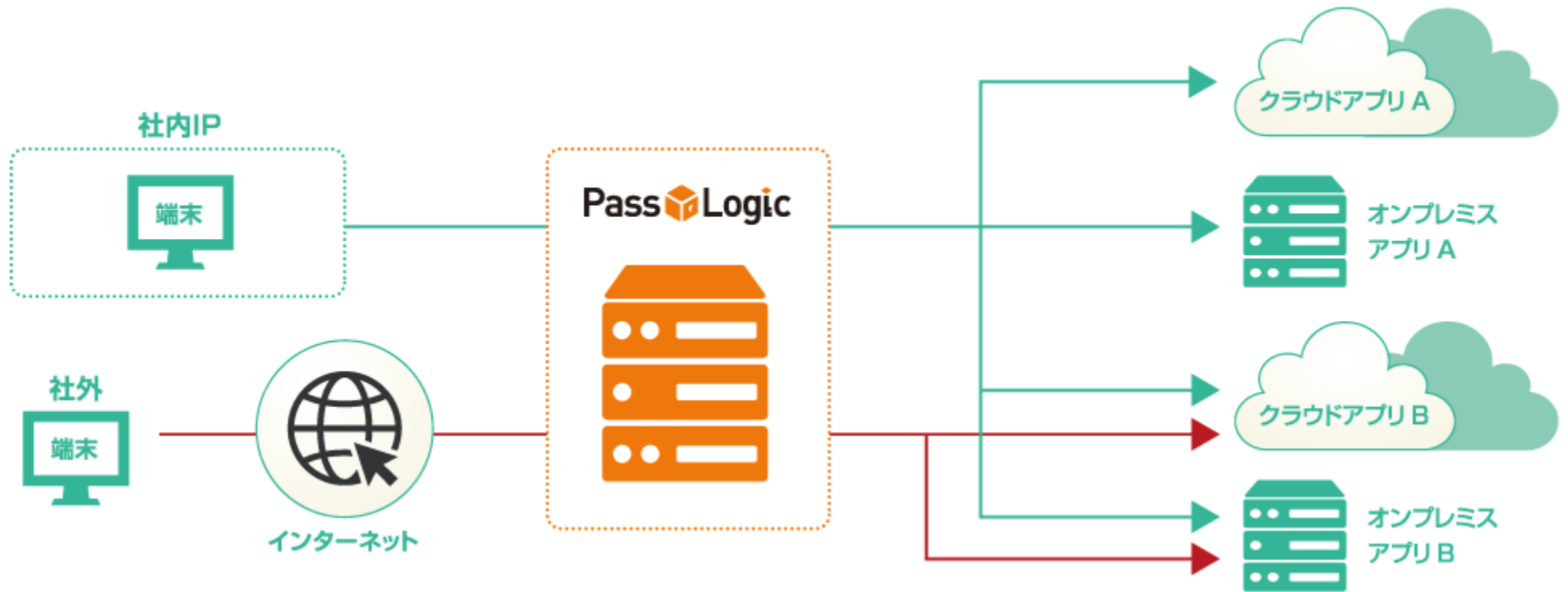
PKI機能（証明書発行・管理機能と認証連携機能）を追加しました。  
トークンレスOTPとの組み合わせで2要素認証が実現します。



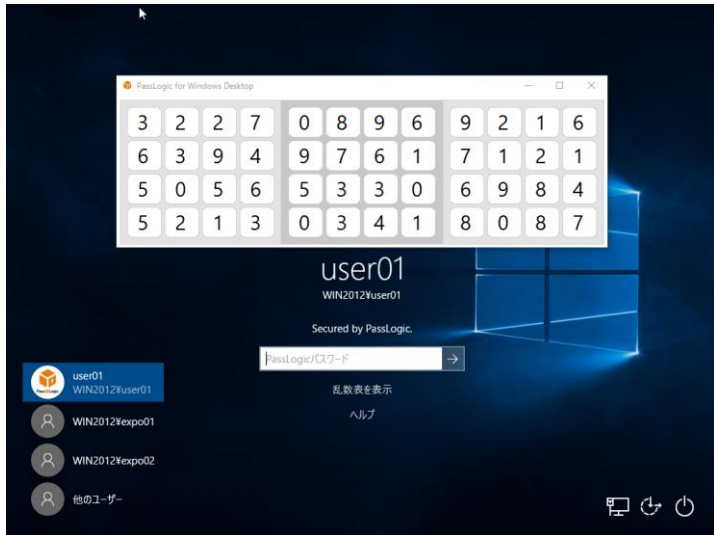
- ポイント1：ハードウェアが不要&マルチデバイスだから、**リモート/モバイルワークと相性抜群！**
- ポイント2：認証サーバ1つで済むので導入・運用コストが低減可能！



IPアドレス制限（WebAPP、Cloud連携）を追加しました。  
例えば、Office365は社内からだけの接続に絞り、salesforceはインターネット経由でどこからでも利用させるといったアクセスコントロールが可能です。

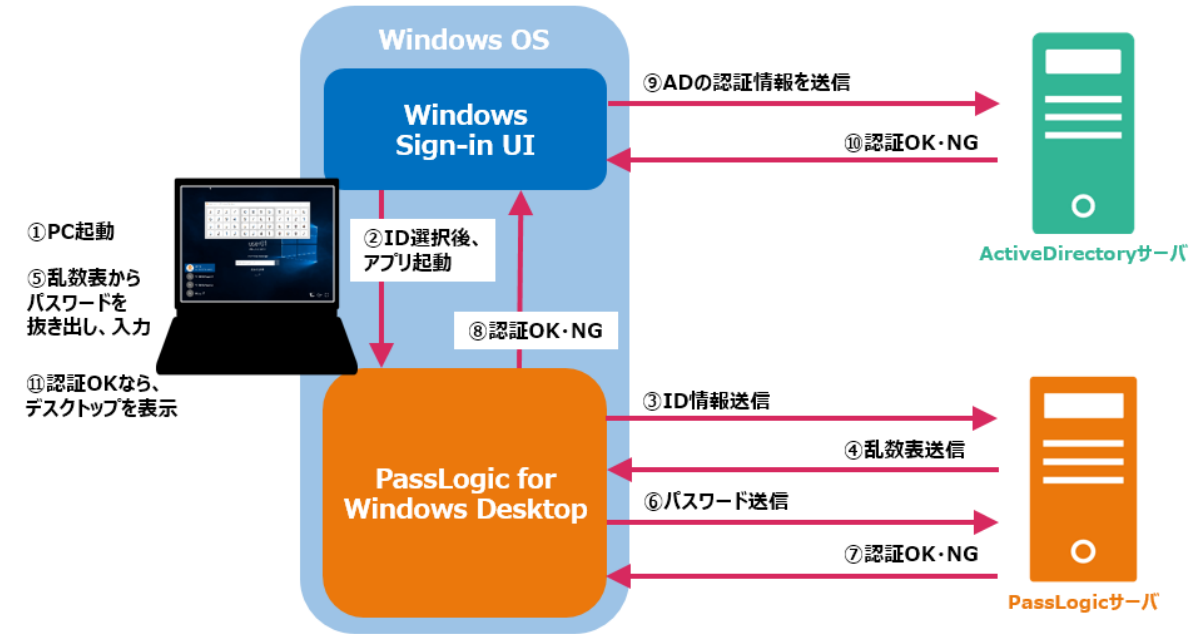


Windowsログオン機能（WindowsのAD連携ユーザのログオン時にPassLogic認証をする機能）を追加しました。



画面はWindows10

## ■ PassLogic for Windows Desktop 利用イメージ図（オンライン時）



|            |   |
|------------|---|
| 正式名称       | PassLogic for Windows Desktop             |
| 対応OS       | Windows 8.1、Windows 10                    |
|            | 32bit / 64bit 両対応                         |
| オフライン認証    | 端末がPassLogicサーバと接続できない状況でもログイン可能な仕組みです。   |
| リモートデスクトップ | リモートデスクトップ（RDP）で接続する際にもPassLogic認証が動作します。 |

機能改善・不具合修正

# 冗長化リカバリ処理の改善 1

冗長構成のリカバリ機能を最適化したことにより、アクセス停止時間を短縮しました。

## リカバリのロジック最適化による改善点

1. データ転送のロジックの見直しにより、リカバリに伴うサービス全断が**10秒～20秒程度**となりました。
2. リカバリ時には、LBなど含めて、PassLogic認証サーバへのアクセスを止める必要がありましたが、v3.0よりこの作業が不要（**PassLogic側での自動対処**）になります。

# 冗長化リカバリ処理の改善 2

冗長構成で、リカバリ実行の際、ファイル管理されている設定情報を含めてリカバリ先にコピーする・しないが選択可能になりました。

## ◆ 管理画面上の表示イメージ

| DB Status |   |
|-----------|---|
| DB 0      | Node Running & Connect ( 192.168.0.248 5439 2 1.000000 )                              |
| DB 1      | Node Down OR Not Connected ( 192.168.0.104 5439 3 0.000000 ) [recovery] [recovery DB] |

[recovery]をクリックした場合

Web ページからのメッセージ ×

? データベースと設定情報を復旧先に送ります。リカバリ手順に従って再インストールと設定は行いましたか？

DB & 設定情報が対象

OK

キャンセル

[recovery DB]をクリックした場合

Web ページからのメッセージ ×

? データベースの情報のみ復旧先に送ります。設定情報はコピーされません。リカバリ手順に従って再インストールと設定は行いましたか？

DBのみが対象

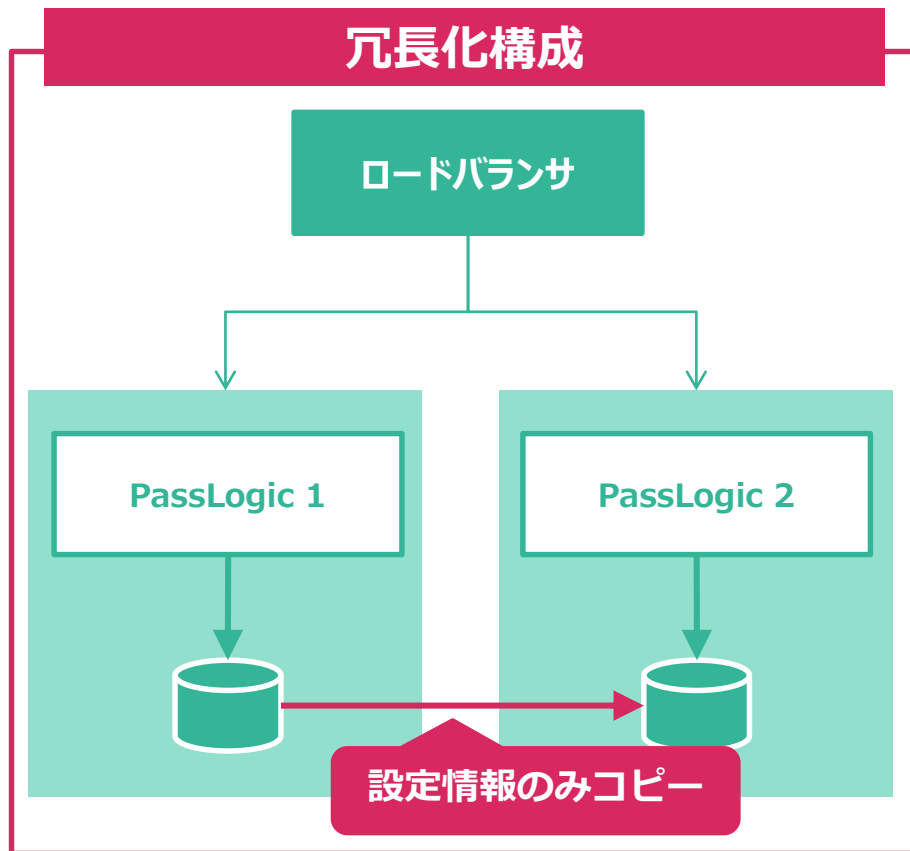
OK

キャンセル

本バージョンより、リカバリ処理をコマンドラインから実行することが可能になっています。

# 冗長化リカバリ処理の改善 3

冗長構成時、ファイル管理されている設定情報のみを冗長先にコピーするコマンドが利用可能になりました。



ポリシー設定や連携設定などを変更した際には、認証サーバ1、認証サーバ2どちらにも設定変更が必要でしたが、今回用意されたコマンドを起動することで冗長先にコピーされるようになります。

# リストア対象の選択

リストアの際にDB情報と設定情報を個別にリストアできるように改善しました。  
PassLogic管理ツール、コマンドラインどちらでもリストアモードを指定できます。

必ずPassLogicからバックアップしたファイルでリストアして下さい。  
他のファイルでリストアすると、システムが正常に動作しなくなります。  
バックアップファイルのサイズが128MBを超える場合はマニュアルに記載の手順でサーバの設定変更が必要です。

バックアップファイル

パスワード

リストアモード

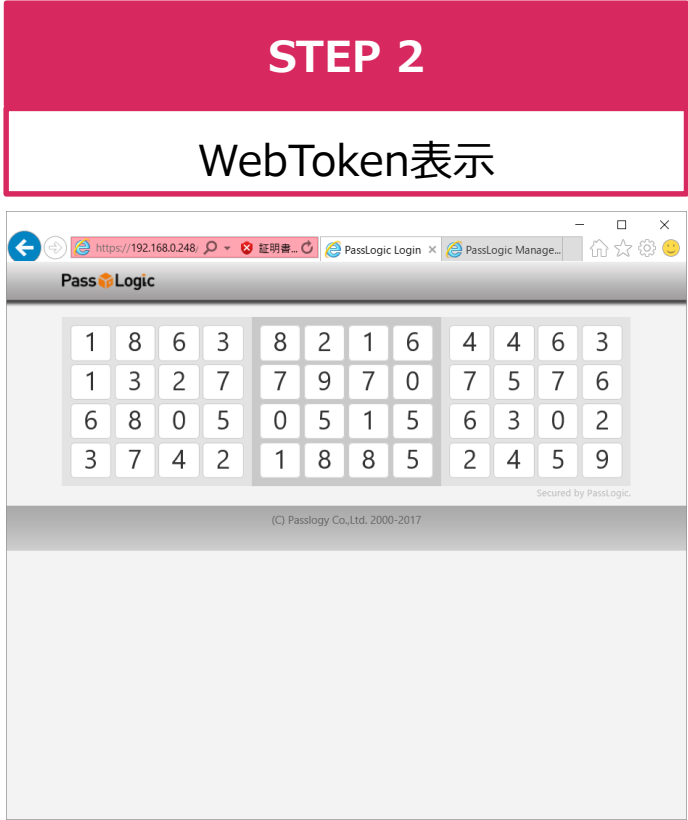
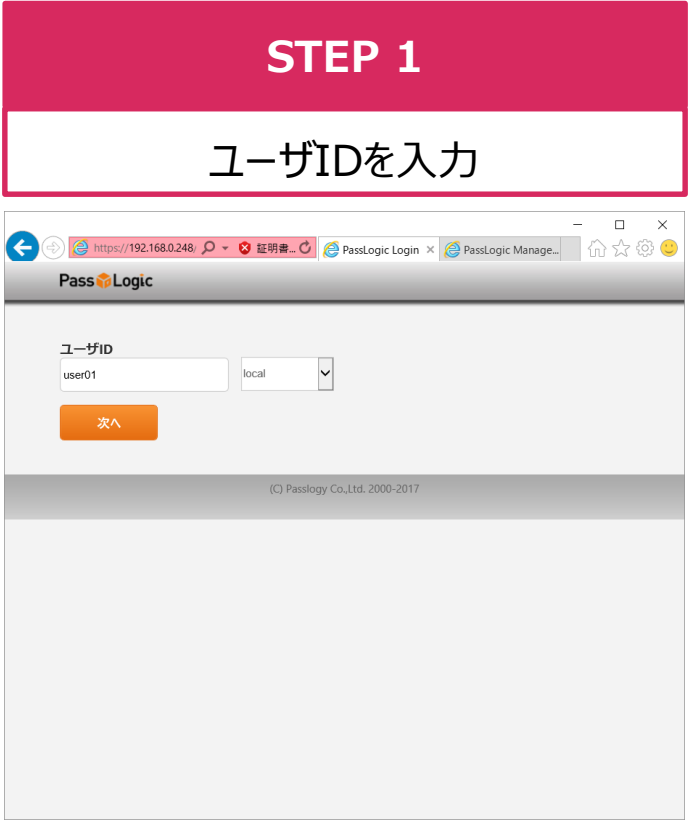
データベースおよび設定情報をリストア  
データベース情報をリストア  
設定情報をリストア

送信

リストア時に対象を指定可能に！

# WebToken利用時もID入力可能になりました。

WebTokenの乱数表表示前にUID入力画面を追加し、個別のWebTokenをユーザで指定して表示できるようになりました。



直接乱数表の画面を表示させることも可能です。



SSL-VPN機器へのシングルサインオンの際に、『特定URLにアクセスして取得するCookie』を要求する仕様に対応できるようになりました。

これによりパルスセキュア社のConnect Secure (旧JuniperMAG) へのシングルサインオンについてもカスタマイズ不要で実現できるようになりました。

# RADIUSアトリビュートによるADパスワード送込に対応

SSL-VPN機器連携の際に、PassLogic上でユーザが入力したADパスワードをRADIUSアトリビュートとして送信できるようになりました。

POSTによるADパスワードの引き渡しは既存機能として実現していましたが、POSTの値を受け取れるVPN機器は多くないため、より容易に引き渡す手段として機能を実装しています。

The screenshot shows the PassLogic administration interface. On the left is a navigation menu with items like 'ユーザ管理', 'ドメイン管理', 'SSL-VPN', 'WebAPP', 'Cloud', '管理者', '設定', 'PKI設定', 'メンテナンス', 'ログ閲覧', and 'パスワード変更'. The main area is titled 'login as admin' and contains a configuration form for RADIUS attributes. The form includes fields for '識別名(\*)' (set to 'vpn'), 'IPアドレス(\*)' (set to '192.168.0.10'), and 'シークレット(\*)' (set to 'secret'). Below these are ten 'ユーザごとのアトリビュート' (User-specific attributes) labeled 'attribute1' through 'attribute10'. The 'AD password' attribute is highlighted with a red callout bubble containing the text: 'LDAP認証連携時 AD Passwordの指定が可能に！' (AD Password specification is possible during LDAP authentication integration!). At the bottom of the form, there is a note: 'ユーザごとにアトリビュートを送信する必要がある場合にアトリビュートの名前(name)を入力します。RFC2865等を参照の上、RADIUSのアクセス許可(Access Accept)パケットに付加できるアトリビュートのみ入力してください。' (When it is necessary to send attributes for each user, enter the attribute name (name). Refer to RFC2865 etc., and enter only attributes that can be added to the RADIUS Access Accept packet.)

PassLogicから受け取ったAD情報を使用して、VPN機器が社内アプリへのシングルサインオンを実現！